REMARKS/ARGUMENTS

Favorable reconsideration of this application, as presently amended and in light of the following discussion, is respectfully requested.

Claims 37-45 are pending in this application. Claims 5-33 are canceled without prejudice or disclaimer, Claims 37, 39 and 41 are amended, and Claims 43-45 are new. The changes to the claims are supported in the originally filed disclosure, including the specification at least from page 30, line 25 to page 33, line 7. No new matter is added.

In the outstanding Office Action, Claims 37-42 were rejected under 35 U.S.C. §112, first and second paragraphs; and Claims 37-42 were rejected under 35 U.S.C. §103(a) as unpatentable over EP 1069567 (Asano) in view of U.S. 2003/0145183 (Muehring) and U.S. 6,212,637 (Ohta).

Initially, regarding the rejections under 35 U.S.C. §112, first and second paragraphs, the Office Action alleges the specification does not describe a plurality of different signatures being created using only a single secret key and message,[1] and further that it is unclear to one of ordinary skill how multiple different signatures can be produced when both the data being signed and a key used to generate the signature are the same.[2] In response, Applicant respectfully submits the claims and specification fully comply with the requirements of 35 U.S.C. §112, first and second paragraphs, as evidenced by the examples discussed below.

The specification describes a processing unit 26 which "uses any message M ..., a random number r(w), and secret key data ... to generate W number of digital signature data SIG(w)."[3] A number W of to be produced disc type recording media is stored in main memory and w = 1, 2, ..., W, and r(w) is an individual random number. Therefore, multiple different signatures are not generated from ***only*** a single secret key and message, as alleged in the Office Action. The language in the claims is open-ended and merely identifies a plurality

[1] Office Action, item 9, page 3.
[2] Office Action, item 12, page 4.
[3] Specification, page 31, lines 20-25, Fig. 3.

of different signature data elements are generated from a secret key data element and a message data element. The language does not preclude the use of, e.g., a random number as noted above and described in the specification. In light of the above comments and the specification, it is respectfully submitted the rejections under 35 U.S.C. §112, first and second paragraphs, should be withdrawn.

As to the cited references, and as previously noted in the response filed October 5, 2009, Claim 37 recites, *inter alia*, a plurality of different identification data elements are generated, where each identification data element includes both (1) a different generated signature data element of the plurality of generated signature data elements and (2) the message data element used in the generation of the different signature data elements. In particular, according to Claim 37, the same message data element is commonly included with different signature data elements to form an identification data for each of a plurality of recording media. It is respectfully submitted the cited references fail to disclose or reasonably suggest these features.

The Office Action acknowledges Asano fails to disclose or suggest the feature of a plurality of different signature elements produced using the same message data, but alleges Ohta describes generating a signature based on data that includes elements which are constants.[4]

Claim 37 requires a common message data, as noted above and in the Office Action. Ohta merely indicates public information can be used in the generation of a signature,[5] where the public information is a prime number of an operation thereof.[6]

The principle of operation of Asano, as described in the response filed October 5, 2009, relies on a data 'm' which is unique for each optical disk[7] for verifying authenticity of a

[4] Office Action, page 6.
[5] Ohta, column 13, lines 25-30.
[6] Ohta, column 12, lines 5 to 25.
[7] In particular, see pages 19-20 of the response filed October 5, 2009.

disk.[8] By replacing the data 'm' of Asano with a prime number of an operation thereof, as suggested in the Office Action in light of the combination with Ohta, the principle of operation of Asano would be destroyed. In particular, Asano would no longer rely on the random physical phenomena of a disk for the basis of authentication. As a result, the device described in Asano would also be unsatisfactory for its intended purpose.

In accordance with MPEP §2143.01.V, the proposed modification (i.e. Ohta modifying Asano) cannot render the prior art unsatisfactory for its intended purpose. Further, in accordance with MPEP §2143.01.VI, the proposed modification cannot change the principle of operation of a relied upon reference. It is respectfully submitted, in light of the above comments, the proposed modification both renders Asano unsatisfactory for its intended purpose and changes the principle of operation of Asano. Accordingly, the rejection of Claim 37 under 35 U.S.C. §103(a) is improper and should be withdrawn.

Although directed at a different statutory class and/or varying in scope, it is respectfully submitted the rejection of Claims 39 and 41 under 35 U.S.C. §103(a) is also improper and should also be withdrawn for substantially the same reasons noted above regarding Claim 37. Therefore, it is respectfully submitted Claims 37, 39 and 41 (and any claims depending therefrom) are allowable over the cited references.

Additionally, Claims 43-45 are new and recite (although directed to different statutory classes and/or varying in scope) the different signature data elements are generated from the secret key data element, the message data element and a different integer selected from a set having a number of integers equal to a number of the different recording media. It is respectfully submitted these features are neither disclose nor reasonably suggested by the art of record and Claims 43-45 are thus further allowable over the art of record by virtue of these features.

[8] Asano, paragraph [0115].

Consequently, in view of the present amendment and in light of the above comments, it is respectfully submitted this application is in condition for allowance. Should the examiner disagree, the examiner is encouraged to contact the undersigned to discuss any remaining issues. Otherwise, an early Notice of Allowance is respectfully requested.

Respectfully submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, L.L.P.

Customer Number
22850

Tel: (703) 413-3000
Fax: (703) 413-2220
(OSMMN 08/07)

Bradley D. Lytle
Attorney of Record
Registration No. 40,073

Marc A. Robinson
Registration No. 59,276